SECURITY ENHANCEMENT FOR UNTRUSTED EXECUTABLE CODE

Publication number: JP2001514411 (T)

Publication date: 2001-09-11

Inventor(s):

Applicant(s):

Classification:

- international: ***G06F12/14; G06F1/00; G06F9/45; G06F21/00; G06F21/22; G06F21/24;*** **G06F12/14; G06F1/00; G06F9/45; G06F21/00; G06F21/22;** (IPC1-7): G06F9/06; G06F12/14

- European: G06F21/00N3E2; G06F21/00N3E1

Application number: JP20000508048T 19980825

Priority number(s): US19970919844 19970828; WO1998US17553 19980825

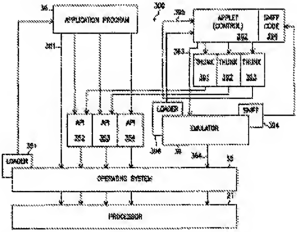
Also published as:

- JP3572016 (B2)
- WO9910795 (A1)
- US6275938 (B1)
- JP2004118866 (A)
- EP1021753 (A1)

more >>

Abstract not available for JP 2001514411 (T)
Abstract of corresponding document: **WO 9910795 (A1)**

Untrusted executable code programs (applets or controls) are written in native, directly executable code. The executable code is loaded into a pre-allocated memory range (sandbox) from which references to outside memory are severely restricted by checks (sniff code) added to the executable code. Conventional application-program interface (API) calls in the untrusted code are replaced with translation-code modules (thunks) that allow the executable code to access the host operating system, while preventing breaches of the host system's security. Static links in the code are replaced by calls to thunk modules. When an API call is made during execution, control transfers to the thrunk, which determines whether the API call is one which should be allowed to execute on the operating system.



Data supplied from the ***esp@cenet*** database — Worldwide